

enabling encrypting a security key to produce an encrypted security key based upon a first biometric key of an authorized user into a token,

enabling determining a second biometric key of a current user of the token based upon a biometric measure of the current user,

enabling decrypting the encrypted security key to produce a decrypted security key based upon the second biometric measure,

enabling the token to receive a challenge parameter, enabling determining an access status based upon the decrypted security key and the response parameter.

20. (TWICE AMENDED) The method of Claim 18, wherein the security key is a first key of a pair of symmetric keys,

the step of determining the response parameter includes the step of encrypting the challenge parameter based upon the second biometric key, and

the step of determining the access status includes the steps of:

decrypting the response parameter to produce a decrypted result based upon a second key of the pair of symmetric keys, and

comparing the decrypted result to the challenge parameter to determine the access status.

REMARKS

Claim 18 has been amended to more clearly define the invention as the invention is claimed in independent Claim 1 and 9. No new matter has been added. No further search or